

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-015960

(43)Date of publication of application : 17.01.2003

(51)Int.Cl. G06F 12/14
G06F 12/00
G11B 20/10
H04L 9/08
H04L 9/32
H04N 5/91

(21)Application number : 2002-070374 (71)Applicant : SONY CORP

(22)Date of filing : 27.09.1996 (72)Inventor : KORI TERUHIKO

(54) FILE GENERATION METHOD AND DATA PROCESSING METHOD

(57)Abstract:

ヘッダ部	プロパティ情報 ・ファイル名 ・ファイル形式 ・データサイズ ・(その他) : ・暗号化された著作権情報
	A/Vデータ本体
データ部	
デリミタ部	ファイルの終了情報

PROBLEM TO BE SOLVED: To make an A/V data file handled on a computer contain copyright information, and to protect the copyright of the A/V data.

SOLUTION: The copyright information, that is composed of file copy generation management information and is encoded with a given encryption key kc, is stored in the header part of the file. When the file is accessed, the copyright information is extracted from the header part at first. If a user who has accessed has not the encryption key kc, the user can not decode the copyright information, and, accordingly, the user can not read the A/V data stored in the file. When the file is copied, the copy generation management information is rewritten and is again stored as the copyright information, and thus the copy generation can be restricted. By encoding the main body of the A/V data with another

encryption key kd and by encoding the key kd together with the copyright information with the key kc, the copyright can be protected more reliably.

(18) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開2003-15960

(P2003-15960A)

(43) 公開日 平成15年1月17日 (2003.1.17)

(51) Int.Cl. ⁷	識別記号	F I	テマコード ⁸ (参考)	
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E	5 B 0 1 7
			3 2 0 B	5 B 0 8 2
12/00	5 3 7	12/00	5 3 7 H	5 C 0 6 3
G 1 1 B 20/10		G 1 1 B 20/10	H	5 D 0 4 4
H 0 4 L 9/08		H 0 4 N 5/91	P	5 J 1 0 4
審査請求 有 請求項の数 6 O L (全 14 頁) 最終頁に続く				

(21) 出願番号 特願2002-70374(P2002-70374)

(62) 分割の表示 特願平8-277130の分割

(22) 出願日 平成8年9月27日 (1996.9.27)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 郡 照彦

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100082762

弁理士 杉浦 正知 (外1名)

最終頁に続く

(54) 【発明の名称】 ファイル生成方法およびデータ処理方法

(57) 【要約】

【課題】 コンピュータ上で扱われるA/Vデータファイルに対して著作権情報を持たせ、A/Vデータの著作権を保護する。

【解決手段】 ファイルのコピーの世代制限情報からなり、所定の暗号化鍵k cによって暗号化される著作権情報が、ファイルのヘッダ部に格納される。このファイルに対してアクセスした場合には、先ず、このヘッダ部から著作権情報が抽出される。アクセスを行なったユーザが暗号化鍵k cを有していなければ著作権情報を復号化できないために、ファイルに格納されたA/Vデータを読み出すことができない。ファイルのコピーの際には、世代制限情報が書き換えられ再び著作権情報として格納されるため、コピーの世代を制限することができる。A/Vデータ本体を別の暗号化鍵k dで暗号化し、鍵k dを著作権情報と共に鍵k cで暗号化することによって、さらに確実に著作権保護を行なうことができる。

ヘッダ部

データ部

デリミタ部

プロパティ情報

・ファイル名

・ファイル形式

・データサイズ

・(その他)

⋮

・暗号化された著作権情報

A/Vデータ本体

ファイルの終了情報

【特許請求の範囲】

【請求項1】 デジタルデータの著作権情報を第1の暗号化鍵に基づき暗号化する第1の暗号化ステップと、上記デジタルデータをデータファイルのデータ部に格納し、上記暗号化した著作権情報を上記データファイルの所定領域に格納してデータファイルを生成するステップとからなることを特徴とするファイル生成方法。

【請求項2】 請求項1に記載のファイル生成方法は、さらに、上記デジタルデータを第2の暗号化鍵で暗号化するステップを有し、上記著作権情報と共に上記第2の暗号化鍵を上記第1の暗号化鍵で暗号化し、上記データファイルの所定領域に格納することを特徴とするファイル生成方法。

【請求項3】 上記暗号化した著作権情報は、上記データファイルのヘッダ部に格納することを特徴とする請求項1に記載のファイル生成方法。

【請求項4】 デジタルデータと、暗号化された該デジタルデータの著作権情報とからなるデータファイルを受信するステップと、上記暗号化されたデジタルデータの著作権情報を復号化し、著作権情報を抽出するステップと、上記著作権情報に基づいて、上記デジタルデータの取り扱いを制御するステップとからなることを特徴とするデータ処理方法。

【請求項5】 上記暗号化されたデジタルデータの著作権情報は、上記データファイルのヘッダ部に格納されていることを特徴とする請求項4に記載のデータ処理方法。

【請求項6】 第2の暗号化鍵で暗号化されたデジタルデータと、第1の暗号化鍵で暗号化された該デジタルデータの著作権情報及び上記第2の暗号化鍵とからなるデータファイルを受信するステップと、上記暗号化されたデジタルデータの著作権情報及び暗号化された第2の暗号化鍵を、第1の暗号化鍵で復号し、著作権情報及び第2の暗号化鍵を抽出するステップと、上記暗号化されたデジタルデータを、上記抽出した第2の暗号化鍵で復号するステップとからなることを特徴とするデータ処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、データファイルの属性情報として著作権情報を持たせ、この著作権情報を所定の方法に基づき暗号化することで、著作物として作成されたデジタルデータの著作権を保護するようなファイル生成方法およびデータ処理方法に関する。

【0002】

【従来の技術】近年、コンピュータの高速化やデジタル記録媒体の大容量化、コンピュータネットワークの発

達、また、画像圧縮技術の発達などが目ざましい。それに伴い、デジタル化された映像信号や音声信号、あるいはコンピュータによって作成されたCG (Computer Graphics) 作品などがA/V (Audio/Video) データファイルとして記録されることが行なわれている。こうして記録されたA/Vデータファイルは、CD-ROMなどに複製され、あるいはネットワークを介して販売ならびに配布される。

【0003】このA/Vデータファイルは、例えばパーソナルコンピュータによって扱われる。そして、ユーザは、このパーソナルコンピュータに接続されたディスプレイ装置やオーディオ装置によってこのA/Vデータファイルを再生して楽しむことができる。

【0004】

【発明が解決しようとする課題】ところで、従来でも、所謂A/V機器において、デジタル化された映像信号や音声信号が記録された記録媒体が扱われていた。A/V機器においては、例えば再生のみ、あるいは記録および再生のみといったように、扱われるA/Vデータに対する機能が限定されていた。したがって、このような、A/V機器において扱われるA/Vデータに対しては、記録媒体に記録されたA/Vデータに対して著作権に関する情報を付加することで、比較的容易に著作権の保護を行なう機構を実現することができた。

【0005】ところが、上述のようなA/Vデータファイルに対しては、このA/V機器において扱われるA/Vデータのように、著作権の保護を行なう機構が導入されていなかった。そのため、このA/Vデータファイルの複写や加工が自由に行われてしまい、著作権の侵害が横行してしまうという問題点があった。

【0006】したがって、この発明の目的は、コンピュータ上で扱われるA/Vデータファイルに対して著作権情報を持たせ、この情報に基づきこのA/Vデータファイルの著作権を保護するようなファイル生成方法およびデータ処理方法を提供することにある。

【0007】

【課題を解決するための手段】この発明は、上述した課題を解決するために、デジタルデータの著作権情報を第1の暗号化鍵に基づき暗号化する第1の暗号化ステップと、デジタルデータをデータファイルのデータ部に格納し、暗号化した著作権情報をデータファイルの所定領域に格納してデータファイルを生成するステップとからなることを特徴とするファイル生成方法である。

【0008】また、この発明は、デジタルデータと、暗号化されたデジタルデータの著作権情報とからなるデータファイルを受信するステップと、暗号化されたデジタルデータの著作権情報を復号化し、著作権情報を抽出するステップと、著作権情報に基づいて、デジタルデータの取り扱いを制御するステップとからなることを特徴とするデータ処理方法である。

【0009】また、この発明は、第2の暗号化鍵で暗号化されたデジタルデータと、第1の暗号化鍵で暗号化されたデジタルデータの著作権情報及び第2の暗号化鍵とからなるデータファイルを受信するステップと、暗号化されたデジタルデータの著作権情報及び暗号化された第2の暗号化鍵を、第1の暗号化鍵で復号し、著作権情報及び第2の暗号化鍵を抽出するステップと、暗号化されたデジタルデータを、抽出した第2の暗号化鍵で復号するステップとからなることを特徴とするデータ処理方法である。

【0010】上述したように、請求項1に記載の発明は、デジタルデータの著作権情報を第1の暗号化鍵に基づき暗号化し、デジタルデータをデータファイルのデータ部に格納し、暗号化した著作権情報をデータファイルの所定領域に格納してデータファイルを生成するようにしているため、第1の暗号化鍵による暗号化を解かない限り、データファイルの所定領域に格納された著作権情報の不正な書き換えが防がれる。

【0011】また、請求項4に記載の発明は、デジタルデータと、暗号化されたデジタルデータの著作権情報とからなるデータファイルを受信し、暗号化されたデジタルデータの著作権情報を復号化し、著作権情報を抽出して、著作権情報に基づいて、デジタルデータの取り扱いを制御するようにしているため、著作権情報の暗号化を解かない限り、デジタルデータを取り扱えないように制御することができる。

【0012】また、請求項6に記載の発明は、第2の暗号化鍵で暗号化されたデジタルデータと、第1の暗号化鍵で暗号化されたデジタルデータの著作権情報及び第2の暗号化鍵とからなるデータファイルを受信し、暗号化されたデジタルデータの著作権情報及び暗号化された第2の暗号化鍵を、第1の暗号化鍵で復号し、著作権情報及び第2の暗号化鍵を抽出して、暗号化されたデジタルデータを、抽出した第2の暗号化鍵で復号するようにしているため、第1の暗号化鍵を持っていないならば、デジタルデータを復号できない。

【0013】

【発明の実施の形態】以下、この発明の実施の一形態について説明する。この発明では、コンピュータ上で扱われるA/Vデータファイルにおいて、属性（プロパティ）情報として著作権情報を持たせる。この著作権情報は、暗号化されて書き込まれるため、ユーザのエディタなどによる書き換えから保護される。この暗号化された著作権情報は、このA/Vデータファイルからデータが読み出される際に参照される。

【0014】図1は、以下の説明において想定するシステム構成を概略的に示す。ここでは、このように、所定のネットワーク2に対して、上述のA/Vデータファイル送出側のコンピュータ1とA/Vデータファイルを受け取る側のコンピュータ3a、3b、・・・とが接続さ

れるシステムが想定される。なお、送出側のコンピュータ1も、受け取り側と同様に、複数接続されることができる。また、これらコンピュータ1および3a、3b、・・・は、所定のOS (Operation System) 上で動作する。詳細は後述するが、このOSは、この実施の一形態における著作権保護システムに対応した機能を有する。

【0015】送出側のコンピュータ1で、所定のアプリケーションソフトウェアA（以下、ソフトウェアAと称する）で作成されたA/Vデータファイルがネットワーク2を介して受け取り側のコンピュータ3a、3b、・・・に受け取られる。そして、例えばコンピュータ3aにおいて、所定のアプリケーションソフトウェアB（以下、ソフトウェアBと称する）を用いてこのA/Vデータファイルが読み出される。なお、ソフトウェアAおよびソフトウェアBとは、同一のアプリケーションソフトウェアであってもよい。

【0016】上述の構成は一例であって、この発明は、例えばDVD (Digital Versatile Disk) - ROMドライブを内蔵したパーソナルコンピュータとデジタルVTRとが接続されたような場合にも適用することができる。

【0017】図2は、この実施の一形態におけるA/Vデータファイル構造の一例を概略的に示す。データは、全体的には一般的なファイル構造を有し、ヘッダ部、データ部、およびデリミタ部とからなる。

【0018】ヘッダ部は、このデータファイルの属性（プロパティ）情報が記される領域である。このプロパティ情報は、ソフトウェアやOSがこのファイルを識別するために必要な情報、例えばこのファイルのファイル名、ファイル形式、およびデータサイズなどの情報からなる。さらに、この一形態においては、このプロパティ情報に、暗号化された著作権情報が含まれる。OSやソフトウェアAあるいはBによってこの著作権情報が読み込まれ、この著作権情報に基づきこのファイルに対する著作権保護がなされる。著作権保護のための著作権情報がファイルのプロパティ情報として格納されるため、この著作権情報は、削除することができない。

【0019】データ部には、A/Vデータ本体、すなわち、音声データおよび/または画像データが格納される。このデータ部には、A/Vデータ本体に限らず、例えばプログラムやスクリプトなどを格納してもよい。また、これらA/Vデータおよびプログラムなどを混在させて格納することもできる。デリミタ部には、例えばこのファイルの終了情報が記される。

【0020】この発明においては、上述の著作権情報は、コピー世代の制限に関する制御情報（CGMS (Copy Generation Management System) と称する）およびアナログビデオ信号に対するコピー制限システムを指示する情報（APS (Analog Protection System) と称する）とからなる。この著作権情報には、これらの情報の他に

も、例えばこのA/Vデータファイルのデータ部に格納されるデータの著作権名、作成日などの、著作権者がそのデータの著作権を主張するために必要な情報や、著作権者の識別を行なう情報、例えば暗証番号やIDを含ませるようにしてもよい。

【0021】CGMS情報およびAPS情報の一例を図3に示す。この図3Aに示すように、CGMS情報は、2ビットのデータからなり、例えば下記のように定義される。

【0022】00：コピー可能

01：未使用

10：コピー1世代可能

11：コピー不可

【0023】このA/Vデータファイルに係わるOSやソフトウェアによって、このCGMS情報が読み出され参照されることによって、このファイルを保存することが可能であるかどうか判断される。

【0024】図4は、CGMSによるコピー世代制限のフローチャートを示す。CGMS情報を含むファイルを例えばコピーしようとした場合、まず、ファイルのヘッダ部が読み込まれ、著作権情報に含まれるCGMS情報が抽出される。そして、次のステップS2において、このCGMS情報が上述の定義のうちのどの状態であるかが判断される。若し、CGMS情報が「00」であれば、処理はステップS5に移行する。そして、ステップS5において、定義に従いこのファイルが保存可能であるとされ、コピーが行なわれファイルが保存される。

【0025】また若し、CGMS情報がファイルのコピーを許可しない「11」であれば、処理はステップS3に移行し、定期に従いファイルが保存不可とされる。

【0026】さらに若し、CGMS情報がファイルの1世代のみのコピーを許可する「10」であれば、処理はステップS4に移行する。ステップS4では、CGMS情報が「10」からファイルのコピーを許可しない「11」に変更される。CGMS情報が変更されると、処理はステップS5に移行し、コピーが行なわれ、ファイルが保存される。CGMS情報が「11」に変更されているため、このファイルはコピー不可とされ、これによりコピーの世代制限がなされる。

【0027】なお、実際には、ファイルのコピーは、例えばファイルの内容が一旦バッファメモリなどに読み込まれ、メモリやディスクなどのデータ記憶媒体の別の領域に書き込まれることによってなされる。したがって、このファイルのコピーは、ファイルの保存と同等に扱うことができる。

【0028】また、図3Bに示すように、APS情報は、上述のCGMS情報と同様に2ビットのデータからなり、例えば下記のように定義される。

【0029】00：APS OFF

01：PSP ON、スプリットバーストOFF

10：PSP ON、2ラインスプリットバーストON
11：PSP ON、4ラインスプリットバーストON
【0030】このAPS情報は、所定の方法で以てアナログビデオ信号に重畳されて、例えば外部のビデオテープレコーダやテレビジョンモニタに送出される。このAPS情報を受け取ったこれらの装置がこのAPSに対応している場合、定義に従い発生されたアナログコピー制限用信号に基づいて生成されたコピー防止用信号によって、このビデオ信号の記録や映出を妨害することができる。

【0031】APS OFFでは、アナログコピー制限用信号を発生しない。PSP ONは、疑似同期信号を含むコピー防止用信号を、アナログビデオ信号に対して重畳するシステムを動作させることを意味する。このシステムを動作させることで、このビデオ信号を供給されたビデオテープレコーダのAGCを誤動作させ、正常な画像の記録を妨害することができる。

【0032】また、スプリットバーストのONは、その一部に反転バースト信号を挿入したカラーバースト信号を、アナログビデオ信号に対して付加するシステムを動作させることを意味する。このシステムを動作させることで、このビデオ信号を供給されたモニタやビデオテープレコーダなどで、APCが正常な動作をすることができず、正常な画像の映出を妨害することができる。スプリットバーストとしては、2ライン単位で反転バースト信号を付加する2ラインスプリットバーストと、4ライン単位で反転バースト信号を付加する4ラインスプリットバーストとの二つの方式が用意され、その一方を選択的に動作させるようになされている。

【0033】図5は、A/Vデータファイルを保存する際の、ソフトウェアA、OS11、およびA/Vデータファイル12間における処理の推移を概略的に示す。A/Vデータファイル12は、例えば当初メモリ（図示しない）上に存在し、ソフトウェアAに対してこのファイル12の保存を指示することによって、このメモリからハードディスクなどの記録媒体（図示しない）に対して保存される。なお、これはこの例に限られず、例えばハードディスクの第1の領域から第2の領域へのA/Vデータファイルのコピー、あるいはネットワークを介して伝送されたA/Vデータの保存などにも適用できる。

【0034】この例に示されるコンピュータにおいて、ソフトウェアによるメモリやハードディスクなどの各種デバイスに対するアクセスは、全てOS11を介してなされる。ソフトウェアAに対して、作成されたA/Vデータファイル12の保存が指示される。この指示は、所定の形式で以てソフトウェアAからOS11に対して伝達される。そして、ソフトウェアAが有する鍵kcがOS11に対して渡される。すると、OS11によって、まず、メモリ上に存在するA/Vデータファイル12の著作権情報が読み出される。後述するが、この著作権情

報は暗号化されているため、所定の方法で以て復号化される。

【0035】 解読された著作権情報からCGMS情報が抽出され、上述の図4に示したフローチャートに従って、このA/Vデータファイル12が保存可能であるかどうか判断される。この判断の結果、保存可能であると判断されたら、このA/Vデータファイル12がハードディスクの所定の領域に書き込まれ保存される。そして、OS11によってこのファイル12の書き込み確認がなされ、確認情報がソフトウェアAに対して伝達され、この情報を受け取ったソフトウェアAにおいて、ファイル12の保存が正しく完了したとされる。

【0036】 ヘッド部に含まれる著作権情報は、ユーザによって、例えばバイナリデータの編集が可能なエディタなどを用いて容易に書き換えられてしまうおそれがある。そこで、この発明においては、上述したように、この著作権情報を所定の方法で暗号化する。図6は、この著作権情報の暗号化の方法の一例を概略的に示す。例えば上述のソフトウェアAでのA/Vデータの作成に伴い、著作権情報が作成される。この著作権情報には、例えば著作権名、データ作成日といった、このファイルに格納されるA/Vデータの著作権を主張するために必要な情報と、上述のCGMS情報とが含まれる。

【0037】 この著作権情報が例えば所定の文字列からなる暗号化鍵kcに基づき暗号化される。暗号化鍵kcは、特定のソフトウェアに依存するもので、例えば、上述のA/Vデータファイルを作成するソフトウェアAや、作成されたファイルを読み込み再生あるいは実行するソフトウェアBに対して入力されたユーザのパスワードPwに基づいて生成される。また、これらのソフトウェアが予めこの鍵kcを有しているとしてもよい。

【0038】 この鍵kcによる暗号化の例として、例えば鍵kcに基づく所定の方法で以て、著作権情報を構成する記号あるいは文字列に対して転字や換字を繰り返して行なう方法が挙げられる。暗号化された著作権情報がヘッド部にプロパティ情報として格納されると共に、作成されたA/Vデータがデータ部に格納され、A/Vデータファイルが作成される。

【0039】 このA/Vデータファイルに含まれる、暗号化された著作権情報は、図7に概略的に示されるように、鍵kcで以て暗号化のときは逆の手順で復号化される。すなわち、例えばソフトウェアBにおいて、A/Vデータファイルのヘッド部に格納されたプロパティ情報が読み出され、このプロパティ情報に含まれる暗号化された著作権情報が抽出される。そして、ソフトウェアBが予め有している鍵kcが用いられ、鍵kcに基づき所定の方法で以て暗号化された著作権情報が復号化される。上述の、CGMSによるコピー世代制限は、この復号化された著作権情報に対してなされる。

【0040】 なお、これら図6および図7に示した著作

権情報の暗号化/復号化の手順は、原理的なものであり、この実施の一形態に適用されるに止まらず、後述する変形例にも適用されるものである。

【0041】 図8は、上述の図6および図7に示した著作権情報の暗号化および復号化の手順を、この実施の一形態に適合させより具体的に示す。この例では、著作権情報を暗号化する際の暗号化鍵kcは、OS11において、ユーザパスワードPwおよびマスク鍵kmとに基づき生成される。

【0042】 ユーザパスワードPwは、例えば、ユーザによって指定される所定の文字列からなり、OS11において、ログインするユーザに対して個別に設定される。また、このパスワードPwは、ソフトウェアAにおいて設定されるようにしてもよい。パスワードPwは、OS11において設定された場合には、OS11の起動毎、ソフトウェアAにおいて設定された場合には、ソフトウェアAの起動毎に、ユーザに対して入力が求められる。マスク鍵kmは、所定の文字列からなり、例えばOS11のコンピュータ1に対するインストールの際になされるユーザ登録によって設定される。

【0043】 OS11によって、A/Vデータファイル12のヘッド部のプロパティ情報から暗号化された著作権情報が読み出される。この著作権情報は、OS11において、上述の鍵kcに基づき復号化される。そして、復号化された著作権情報からCGMS情報が抽出され、このCGMS情報に基づきこのファイル12の保存の禁止/許可が判断される。

【0044】 この場合、復号化された著作権情報に基づきこのファイル12に対するアクセスそのものの禁止/許可を判断するようにもできる。これは、例えば、パスワードPwがソフトウェアAに対して設定された場合には、この著作権情報がソフトウェアAに渡され、ソフトウェアAにおいてパスワードPwとこの著作権情報とが照合され、その結果がOS11に渡されることによってなされる。

【0045】 一方、ソフトウェアAにおいて作成されたA/Vデータに対してCGMS情報が設定され、A/Vデータファイルとして保存される際に、OS11において、鍵kcに基づいて著作権情報の暗号化がなされる。

【0046】 この実施の一形態では、A/Vデータファイルの著作権保護のためのCGMS情報の、例えば照合や書き換えといった処理は、OS11においてなされる。このOS11上では、作成される全てのファイルに対して著作権情報が設定され、全てのファイル操作の際に、この設定された著作権情報の照合などの処理がなされる。そこで、この著作権保護システムに対応していない、他のOS上で作成されたファイル操作に対して互換性を持たせる必要がある。

【0047】 図9は、このファイルの互換性を考慮した、OS11におけるファイルに対するアクセスのプロ

ーチャートを示す。ファイルに対するアクセスがなされると、まず、ステップS10において、このファイルがOS11による著作権保護システムに対応しているかどうか判断される。この判断は、例えば、OS11において著作権保護システムに対応しているファイルにはヘッダ部にその旨を示すフラグなどを記し、このフラグの有無を調べることによって行なうことができる。また、ヘッダ部の著作権情報そのものの有無を調べるようにしてもよい。

【0048】若し、著作権保護システムに対応していないと判断されたら、このファイルに対する著作権保護の手段はとられず、ステップS17においてファイルの保存がなされる。

【0049】一方、ステップS10でファイルが著作権保護システムに対応していると判断されたら、処理はステップS11に移行する。そして、ステップS11において、このファイルの著作権情報が読み出され、復号化される。この復号化は、例えばOS11から所定のソフトウェア（例えば上述のソフトウェアAあるいはB）に対して暗号化鍵kcを要求し、この要求に対してそのソフトウェアから渡された鍵kcに基づいてなされる。著作権情報の復号化がなされると、処理はステップS12に移行する。

【0050】ステップS12では、復号化された著作権情報からCGMS情報が抽出される。そして、次のステップS13で、CGMS情報の状態が判断される。若し、CGMS='11'であれば、処理はステップS14に移行し、上述のCGMSの定義に従いファイル保存は不可であるとされる。また若し、CGMS='00'であれば、定義に従いファイル保存が可能とされるため、処理はステップS16に移行する。さらに若し、CGMS='10'であれば、処理はステップS15に移行し、CGMS情報が'11'に書き換えられる。そして、処理は次のステップS16に移行する。

【0051】ステップS16において、著作権情報が暗号化される。この暗号化は、例えばOS11から所定のソフトウェアに対して暗号化鍵kcを要求し、この要求に対してそのソフトウェアから渡された鍵kcに基づいてなされる。暗号化がなされると、ファイルのヘッダ部に含まれる著作権情報がこのステップS16で暗号化された著作権情報とされる。そして、次のステップS17で、このファイルが保存される。

【0052】なお、上述の説明では、ネットワーク2に接続されたコンピュータ1および3a、3b、・・・のそれぞれには、全て同一のOS11が搭載されているとしたが、これはこの例に限定されない。コンピュータ1および3a、3b、・・・に対してそれぞれ異なるOSが搭載されている場合でも、互いに共通のプロトコルでデータ通信を行なうことができれば、この発明による著作権保護システムを適用することができる。

【0053】また、上述のフローチャートは、著作権保護システムに対応していないファイルの互換性が考慮されたものだが、この処理を応用することによって、著作権保護を必要とされないファイルを選択的に設定することができる。

【0054】A/Vデータファイルは、データファイルとしてのコピーが行なわれるだけでなく、例えばコンピュータによってこのファイルが再生あるいは実行され、アナログ方式やデジタル方式のビデオ信号とされ外部に出力されることも考えられる。この出力されたビデオ信号は、例えばアナログビデオテープレコードによって記録され、それによりA/Vデータに対する著作権の侵害が生じる可能性がある。したがって、このような場合における著作権保護についても考慮する必要がある。

【0055】図10は、A/Vデータファイルから再生されたA/Vデータがコンピュータ外部に対して出力される場合の、データ変換の方法を概念的に示す。ここでは、A/VデータがアナログRGB信号に変換され出力される例を示す。図示せずとも、ソフトウェアAによってA/Vデータファイル12が再生され、A/Vデータが出力される。このA/Vデータは、エンコード20に供給され、D/A変換されると共に、例えばRGBの各色の信号からなるコンポーネントビデオ信号とされる。このコンポーネントビデオ信号のうち、例えばR信号が加算器22の一方の入力端に対して供給される。

【0056】この加算器22は、他方の入力端に供給された信号の、一方の入力端に供給されたビデオ信号に対する加算を、ビデオ信号に同期して所定のタイミングで制御することができる。これは、例えばエンコード20において、A/Vデータをビデオ信号に変換する際に用いられたタイミング信号に基づき生成された制御信号が、この加算器22に供給されることによってなされる。

【0057】一方、ソフトウェアAあるいはOS11によって、A/Vデータファイルから著作権情報が読み出される。この著作権情報が鍵kcによって復号化され、APS情報が抽出される。そして、このAPS情報に基づきアナログコピー制限用信号が生成され、生成されたこの信号は、加算器22の他方の入力端に供給される。加算器22では、この信号を、一方の入力端に供給されているR信号の、例えば垂直ブランキング期間に加算する。

【0058】図示しないが、このアナログビデオ信号は、モニタに対して供給され映出されると共に、例えばAPSに対応したRGB信号/コンポジットビデオ信号変換器に供給される。コピー制限用信号は、ブランキング期間に重畳されているため、モニタへの映出には直接的な影響はない。しかしながら、APSに対応したRGB信号/コンポジットビデオ信号変換器を介して外部にコンポジットビデオ信号として出力された場合、上述の

図3Bに一例が示される、APS情報の定義に基づいたコピー防止用信号がこのビデオ信号に対して重畳または付加される。そのため、このビデオ信号をビデオテープなどに記録しても、正常な画像として再生することができず、結果的にA/Vデータに対する著作権を保護することができる。

【0059】なお、A/Vデータファイルが再生されデジタル画像データとして外部に出力される場合には、著作権情報から抽出されたCGMS情報およびAPS情報とがそのまま伝送され、例えばデジタルビデオカセットレコーダによって、テープの所定の領域に記録される。したがって、この場合でも容易にコピー防止の効果を得ることができる。

【0060】次に、この発明の実施の一形態の変形例について説明する。図11は、この変形例におけるA/Vデータファイル構造の一例を概略的に示す。この変形例においては、データ部に格納されたA/Vデータが所定の暗号化鍵k_dに基づき暗号化され、この鍵k_dがA/Vデータファイルのヘッダ部の著作権情報と共に、所定の暗号化鍵に基づき暗号化される。この変形例では、このようにA/Vデータそのものを暗号化することにより、より強固にA/Vデータの著作権保護を行なうものである。

【0061】図12は、この変形例によるA/Vデータファイルの暗号化の方法の一例を概略的に示す。この例においては、A/Vデータファイル供給側からユーザに対して配布される顧客管理鍵k_uを用いて、著作権情報およびデータ暗号化鍵k_dの暗号化を行なう。

【0062】A/Vデータは、このデータの供給側で管理しているデータ暗号化鍵k_dに基づいて暗号化される。この暗号化には、例えば、鍵k_dに基づいた所定の規則に従って転字や換字を繰り返すことによってなされる。この暗号化されたA/Vデータは、A/Vデータファイルのデータ部に格納される。また、このA/Vデータの暗号化に用いられた鍵k_dは、著作権情報と共に、A/Vデータの供給側において管理される顧客管理鍵k_uに基づき暗号化される。この顧客管理鍵k_uは、例えばこのA/Vデータの供給を受けた顧客のそれぞれに対して設定され、A/Vデータ供給側から渡される。こうして暗号化された著作権情報および鍵k_dとは、プロパティ情報としてA/Vデータファイルのヘッダ部に格納される。

【0063】図13は、この変形例によるA/Vデータファイルの復号化の方法の一例を概略的に示す。A/Vデータの供給側からユーザに対して渡されたA/Vデータファイルにおいて、ヘッダ部が読み込まれ、暗号化された著作権情報およびデータ暗号化鍵k_dが抽出される。また、A/Vデータ供給側からユーザに対して、予め顧客管理鍵k_uが渡される。ヘッダ部から抽出された暗号化された著作権情報および鍵k_dがこの顧客管理鍵

k_uによって復号化される。そして、この復号化された顧客管理鍵k_uによって、データ部に格納された、暗号化されたA/Vデータが復号化される。

【0064】この例のように、顧客管理鍵k_uを用いることによって、A/Vデータ供給側は、ユーザに対してA/Vデータファイルの使用を限定することができ、A/Vデータ供給側における顧客管理を行なうことができる。そのため、この顧客管理鍵k_uを用いた方法は、例えば大量生産されるA/Vデータファイルに対して用いて好適なものである。

【0065】一方、上述の実施の一形態における著作権保護の方法は、例えば個人の創作に関する著作権の保護に対して用いて好適である。

【0066】なお、この変形例は、この例に限らず、例えば顧客管理鍵k_uの代わりに、上述の実施の一形態において用いられた暗号化鍵k_cを用いることも可能である。勿論この場合には、A/Vデータ供給側による顧客管理は、厳密には行なわれない。

【0067】上述の実施の一形態およびその変形例においては、著作権情報処理に対応したOSに対してこの発明が適用されるように説明したが、これは、この例に限定されるものではない。図14は、この発明の別の変形例として、著作権情報処理に対応していないOSに対してこの発明が適用された際の、ソフトウェアA'、OS11'、A/Vデータファイル12間における処理の推移を概略的に示す。なお、この別の変形例は、上述の実施の一形態およびその変形例とによる何方のファイル構造に対しても適用可能なものである。

【0068】この別の変形例においては、上述の実施の一形態およびその変形例ではOS11においてなされていた、A/Vデータファイルからの著作権情報の読み出しおよび読み出された著作権情報の解読を、ソフトウェアA'上で行なう。A/Vデータファイル12は、当初図示されないメモリ上に存在し、ソフトウェアA'に対してこのファイル12の保存を指示することによって、このメモリから例えば図示されないハードディスクに対して保存される。なお、これはこの例に限られず、例えばハードディスクの第1の領域から第2の領域へのA/Vデータファイルのコピー、あるいはネットワークを介して伝送されたA/Vデータの保存などにも適用できる。

【0069】ソフトウェアA'に対して、作成されたA/Vデータファイル12の保存が指示される。この指示に基づき、A/Vデータファイル12のヘッダ部からプロパティ情報が読み出され、読み出されたこのプロパティ情報から著作権情報が抽出される。この著作権情報は、例えばソフトウェアA'が固有に有している暗号化鍵k_cによって暗号化されている。この鍵k_cに基づき著作権情報が復号化され、解読される。

【0070】なお、著作権情報の暗号化に用いられた暗

号化鍵は、この例のような暗号化鍵k cに限られない。例えば、上述の、A/Vデータファイル供給側からユーザに対して渡された顧客管理鍵k uをこの暗号化鍵として用いるようにもできる。

【0071】解説された著作権情報からCGMS情報が抽出され、上述の図4に示したフローチャートに従って、このA/Vデータファイル12が保存可能であるかどうか判断される。この判断の結果、保存可能であると判断されたら、OS11'によって、このA/Vデータファイル12が例えばハードディスクの所定の領域に書き込まれ保存される。そして、OS11'によってこのファイル12の書き込み確認がなされ、確認情報がソフトウェアA'に対して伝達され、この情報を受け取ったソフトウェアA'において、ファイル12の保存が正しく完了したとされる。

【0072】

【発明の効果】以上説明したように、この発明によれば、A/Vデータファイルのプロパティ情報に、著作権保護を行なうための著作権情報が含まれる。そのため、コンピュータ上で扱われるA/Vデータに対しても、著作権保護の機構を導入することができ、著作権の侵害が防止される効果がある。

【0073】また、この発明によれば、著作権情報に対してコピーの世代制限を制御するCGMS情報が含まれ、デジタルA/V機器などで既に導入されているものと同一の概念でA/Vデータの著作権保護が行なわれる。そのため、コンピュータ上のA/VデータとデジタルA/V機器との間で、著作権保護の考え方に整合性がとれる効果がある。

【0074】さらに、この発明によれば、著作権情報は、暗号化されているため、ユーザによる不正な書き換えなどから保護され、安全性が高いという効果がある。

【0075】さらにまた、この発明によれば、OSにおいてファイルの更新や保存の際に著作権情報が含まれるプロパティ情報を参照するようにされているため、アプリケーションソフトウェアだけで同様の処理を行なう場合に比べ、著作権保護の確実性がより高まるという効果がある。

【0076】また、この発明による著作権保護のための処理は、高々数バイトのデータをソフトウェアあるいはOS上でハンドリングするだけで行なわれるので、著作権保護のために新たに発生するコストは無視できる程度のものであるという効果がある。

【0077】さらに、この発明による著作権情報は、A/Vデータファイルのプロパティ情報として扱われるため、ファイルから削除することができず、より確実に著

作権保護を行なうことができるという効果がある。

【0078】また、この発明による著作権情報は、既に存在するデジタルA/V機器における著作権保護と共通の考えに基づいて設定されている。そのため、この発明によるA/Vデータは、デジタルA/V機器とのインターフェイス上にそのまま伝送することができるという効果がある。

【図面の簡単な説明】

【図1】説明において想定されるシステム構成を概略的に示す図である。

【図2】実施の一形態におけるA/Vデータファイル構造の一例を概略的に示す図である。

【図3】CGMS情報およびAPS情報の一例を示す略線図である。

【図4】CGMSによるコピー世代制限のフローチャートである。

【図5】A/Vデータファイルを保存する際の、ソフトウェア、OS、およびA/Vデータファイル間における処理の推移を概略的に示す図である。

【図6】著作権情報の暗号化の方法の一例を概略的に示す図である。

【図7】著作権情報の復号化の一例を概略的に示す図である。

【図8】著作権情報の暗号化および復号化の手順をより具体的に示す図である。

【図9】ファイルの互換性を考慮した、OSにおけるファイルに対するアクセスのフローチャートである。

【図10】A/Vデータファイルを外部出力する場合のデータ変換の方法を概念的に示す図である。

【図11】変形例におけるA/Vデータファイル構造の一例を概略的に示す図である。

【図12】顧客管理鍵k uを用いた場合の、A/Vデータファイルの暗号化の方法の一例を概略的に示す図である。

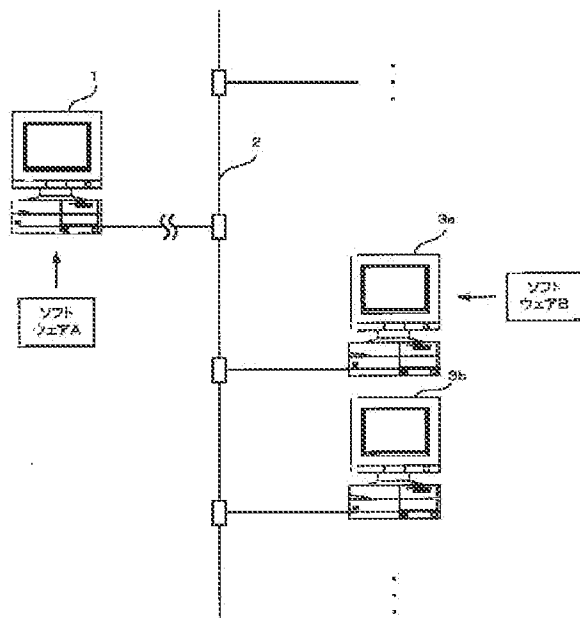
【図13】顧客管理鍵k uを用いた場合の、A/Vデータファイルの復号化の方法の一例を概略的に示す図である。

【図14】OSが著作権情報処理に対応していない場合の、ソフトウェア、OS、A/Vデータファイル間における処理の推移を概略的に示す

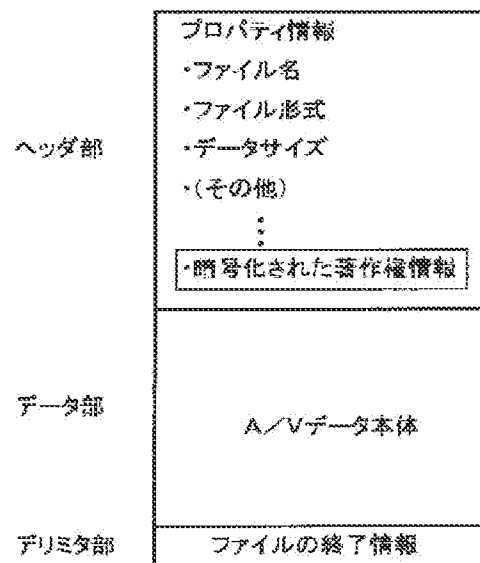
【符号の説明】

1, 3 a, 3 b・・・コンピュータ、11・・・OS、12・・・A/Vデータファイル、A, B・・・アプリケーションソフトウェア、k c・・・暗号化鍵、k d・・・データ暗号化鍵、k m・・・マスク鍵、k u・・・顧客管理鍵、Pw・・・ユーザパスワード

【図1】



【図2】



【図3】

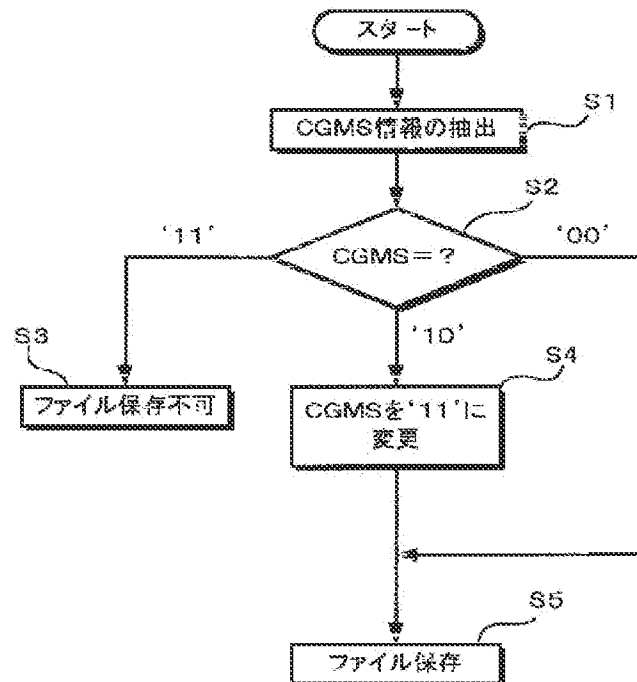
A

CGMS		定義
1	1	コピー不可
1	0	コピー1世代可能
0	1	未使用
0	0	コピー可能

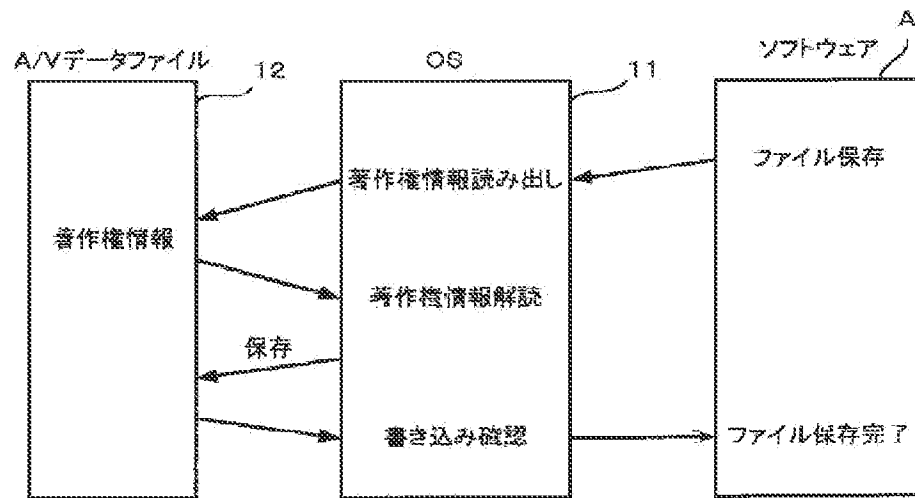
B

フラグ		定義
0	0	OFF
0	1	FSP ON
1	0	FSP ON, 25インスピリットバーストON
1	1	FSP ON, 45インスピリットバーストON

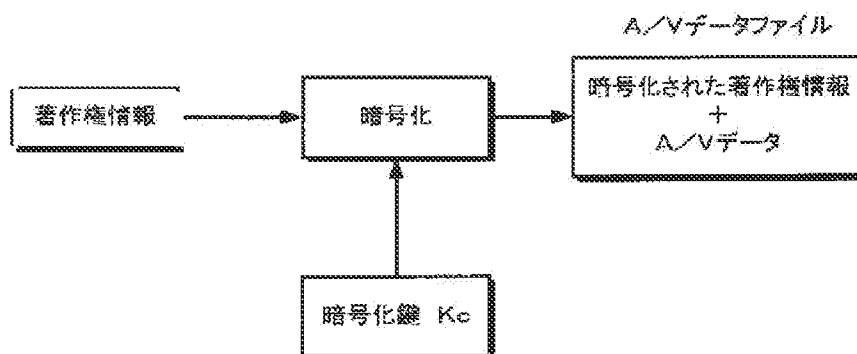
【図4】



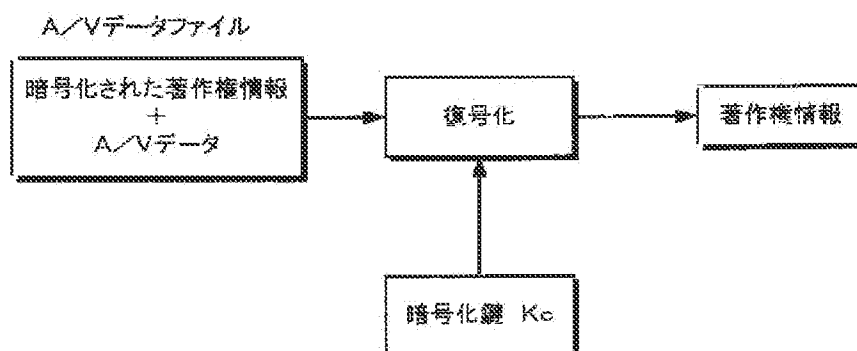
【図5】



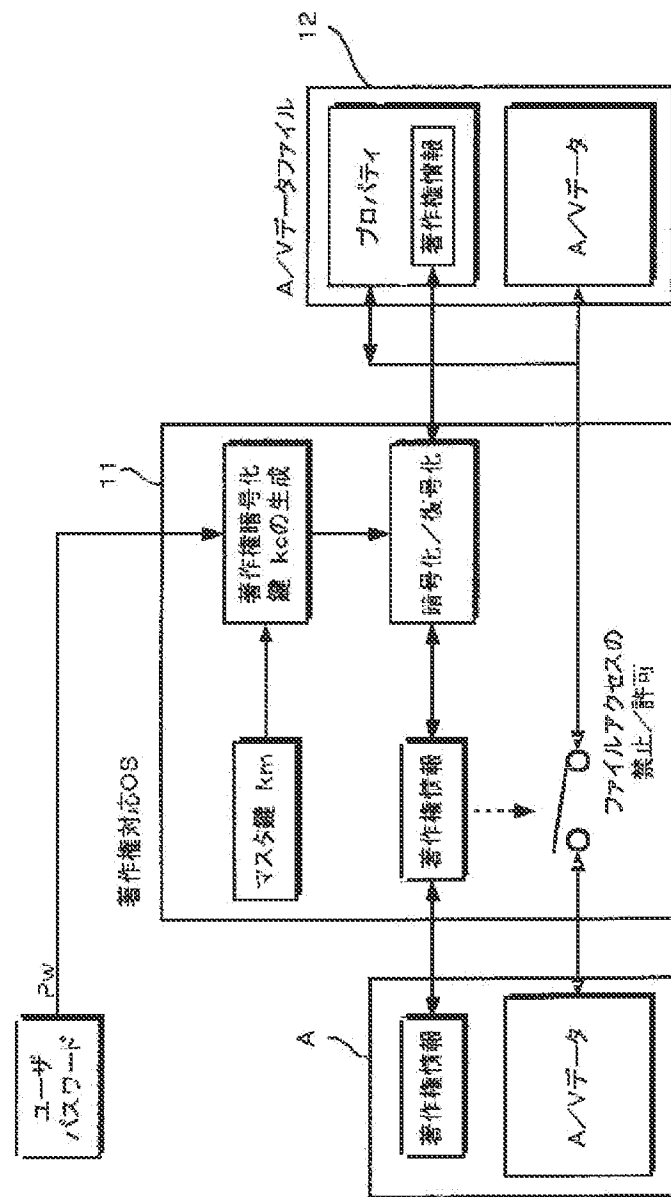
【図6】



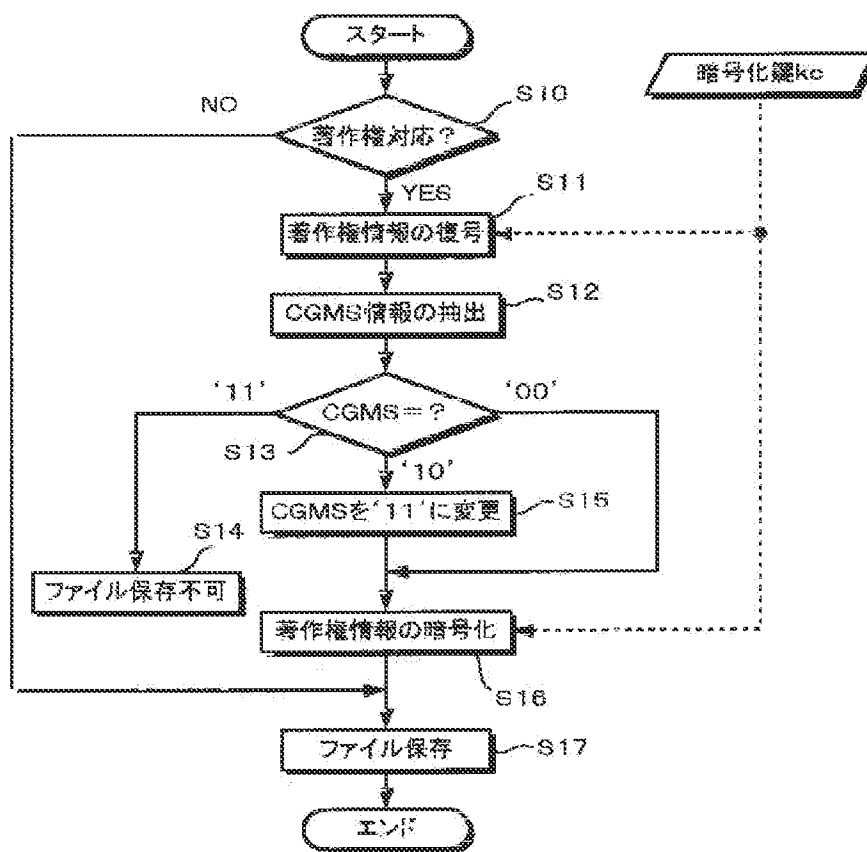
【図7】



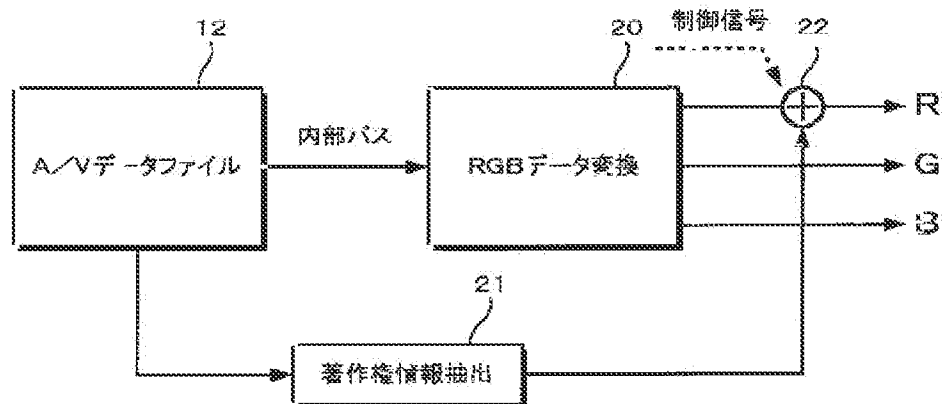
【図8】



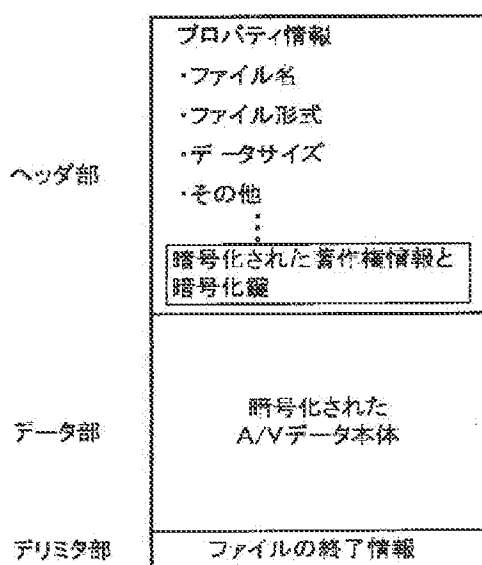
【図9】



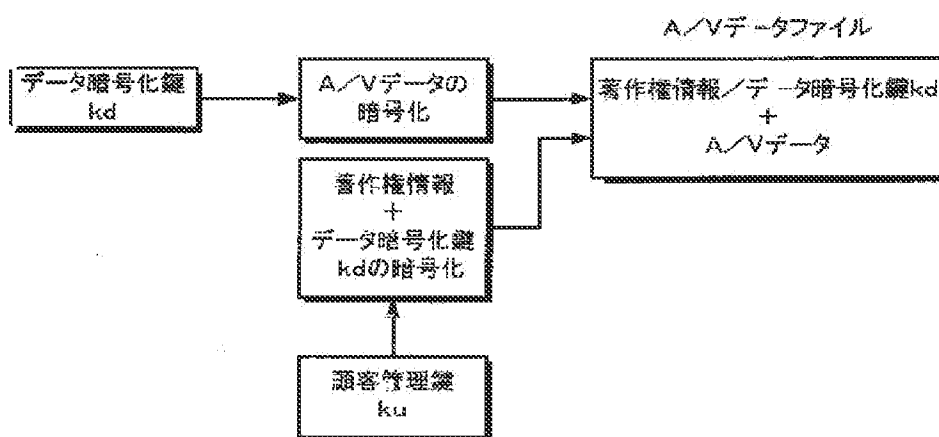
【図10】



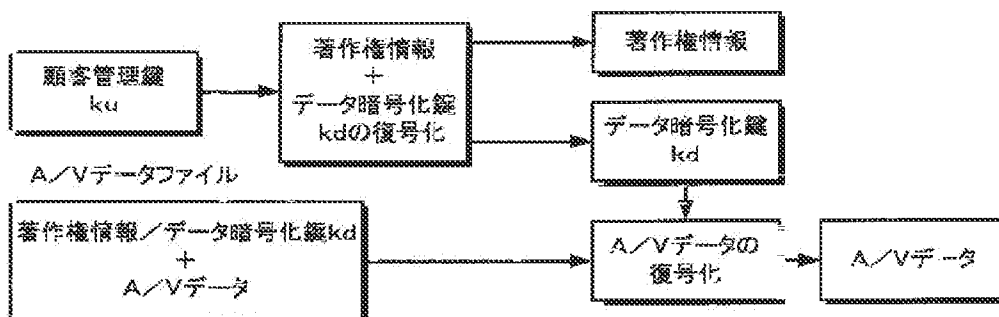
【図11】



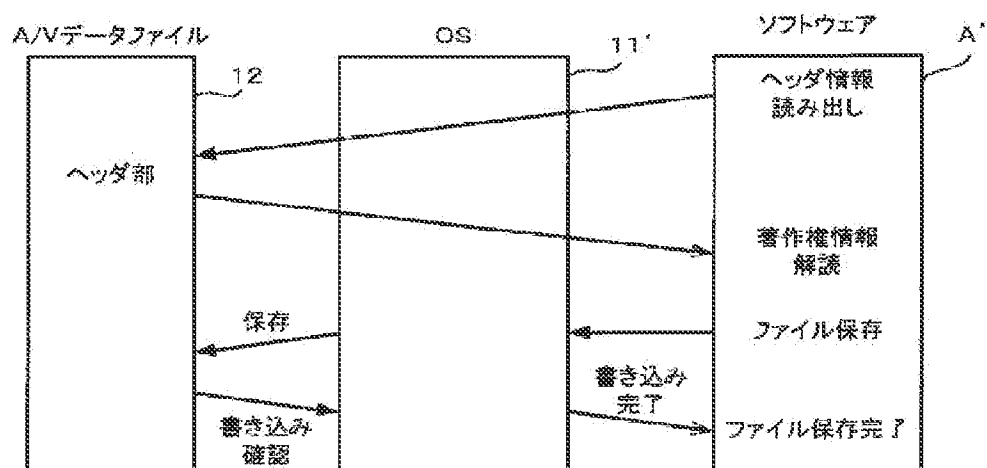
【図12】



【図13】



【例 14】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	(参考)
----------------------------	------	-----	------

H O 4 L 9/32

H O 4 N 5/91

識別記号

FI

H04L 9/00

601A

671

(参考)

Fターム(参考) 5B017 AA03 BA07 CA09 CA16

5B082 EA11 GA11

5C053 FA13 FA24 GB06 JA21 LA11

5D044 AB05 AB07 BC02 CC04 DE49

DE50 DE53 EF05 FG18 GK17

HLOS

5J104 AA15 AA16 EA17